



Lower Bounds on the Broadcasting and Gossiping Time of Restricted Protocols

Michele Flammini, Stéphane Pérennes

► To cite this version:

Michele Flammini, Stéphane Pérennes. Lower Bounds on the Broadcasting and Gossiping Time of Restricted Protocols. RR-3612, INRIA. 1999. inria-00073066

HAL Id: inria-00073066

<https://inria.hal.science/inria-00073066>

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Lower Bounds on the Broadcasting and Gossiping Time of Restricted Protocols

Michele Flammini — Stéphane Pérennès

N° 3612

janvier 1999

THÈME 1



***rapport
de recherche***

Lower Bounds on the Broadcasting and Gossiping Time of Restricted Protocols

Michele Flammini* , Stéphane Pérennès†

Thème 1 — Réseaux et systèmes
Projet sloop

Rapport de recherche n° 3612 — janvier 1999 — 27 pages

Abstract: In this paper we extend the technique provided in [6] to allow the determination of lower bounds on the broadcasting and gossiping time required by the so-called “restricted” protocols. Informally, a protocol is (i, o) -restricted at a given processor if every outgoing activation of an arc depends on at most i previous incoming activations and any incoming activation influences at most o successive outgoing activations. Examples of restricted protocols are those running on bounded degree networks or systolic.

We thus derive improved lower bounds on the broadcasting time in several well-known networks, such as Butterfly, de Bruijn and Kautz graphs.

Moreover, we derive the first general lower bound on the gossiping time of d -bounded degree networks in the directed and half-duplex cases. Improved lower bounds on gossiping are also obtained for Butterfly, de Bruijn and Kautz graphs.

Finally, as a corollary we obtain the same lower bounds on s -systolic protocols obtained in [6].

All the results are also extended to other communication models, such as c -port and/or postal and optical.

Key-words: Broadcasting, Gossiping, bounded degree networks, systolic protocols

Work supported by the EU ESPRIT Long Term Research Project ALCOM-IT under contract N. 20244 and by the SLOOP project I3S-CNRS /INRIA /Univ. Nice–Sophia Antipolis.

* Dipartimento di Matematica Pura ed Applicata, Università di L'Aquila, via Vetoio Loc.Coppito, I-67010 L'Aquila, Italy. E-mail: flammini@univaq.it

† SLOOP I3S-CNRS/INRIA/Université de Nice–Sophia Antipolis, 2004 Route des Lucioles, BP 93, F-06902 Sophia-Antipolis Cedex, France. E-mail: speren@sophia.inria.fr

Bornes inférieures du temps de diffusion de protocoles contraints

Résumé : Nous généralisons les techniques introduites dans [6] afin de minorer le temps de diffusion et d'échange total de protocoles satisfaisant certaines contraintes. Intuitivement un protocole est (i, o) *contraint* si un message émis dépend uniquement des i derniers messages reçus et si un message reçu influence au plus les o envois suivants. Cette contrainte est utile car elle apparaît à la fois dans le cas des protocoles systoliques, et des protocoles fonctionnant dans des réseaux de degré borné.

Les résultats sont appliqués afin de déterminer de nouvelles bornes inférieures pour la diffusion et l'échange total dans des réseaux «classiques». Nous retrouvons aussi les résultats de [6] et prouvons la première borne inférieure non triviale sur le temps de l'échange total dans les réseaux de degré borné.

Enfin nous montrons comment la technique introduite peut s'appliquer à des modèles de communication divers (modèles postal ou optique)

Mots-clés : Diffusion, Échange total, Réseaux de degré borné, protocoles systoliques

1 Introduction

Broadcasting (one-to-all) and gossiping (all-to-all) are well known communication primitives to disseminate information in communication networks. Such problems have been extensively investigated in recent years for many different networks and under a large variety of models. A survey of the main related results can be found in [8, 7, 4, 11, 9, 10]

We consider first the basic model, called whispering or processor-bounded, where at each communication round each processor can have only one active incident link, i.e. the set of the active links forms a matching. Active links are used at the corresponding processors to deliver the items known till that communication round to their neighbors. If the network can be modeled as an undirected graph, for gossiping it is possible to further distinguish between two different cases: the half-duplex mode, in which active links allow the transmission of messages only in one direction, and the full-duplex mode, in which messages can travel in both directions simultaneously. Clearly such a distinction is meaningless for broadcasting, as there is always a single item traveling around and it traverses each link only once and in one direction.

Starting from the basic whispering model, several generalizations can be defined. First, it is possible to relax the constraint that at each communication round only an incident link is activated, thus allowing at most $c \geq 1$ active links. This model is called c -port. Moreover, in the postal model it is assumed that the communication time can be slower than one time step, so that when items are sent through an active link, they will be available at the arriving processor only after a number of rounds $\delta \geq 1$. On the other hand, in the optical model communication time is faster than processors speed, so that when items arrive have to wait a fixed number $\delta \geq 0$ of steps before they can be sent to other processors. Notice that the above models are orthogonal in the sense that it is possible to have c -port also in the postal and optical cases. Finally, it is possible to establish some bounds on the lengths of the messages, i.e. on the number of items that can travel simultaneously on a link. However, all the results shown in this paper assume no bound on the messages length.

A more detailed and exhaustive description of the various models together with the corresponding results can be found in [8, 7, 4, 11, 9, 10, 2]

Let us now consider the whispering model. The best lower bounds on the broadcasting time are as follows. Let the parameter d be defined for undirected graphs as the maximum degree minus one and for directed graphs as the maximum out-degree. Then for bounded-degree networks in [16, 3] it has been proved that the broadcasting time $b(G)$ of a graph G of n vertices with parameter d satisfies

$b(G) \geq e(d) \log n$, where $e(2) = 1.4404$, $e(3) = 1.1374$, $e(4) = 1.0562$ and for large d $e(d) \approx (1 + (\log e)/2^d)$ (from now on all logarithms are assumed in base 2).

For Butterfly and de Bruijn networks better lower bounds have been obtained by using their structure in [13] and recently improved in [18, 17]. For example in [18] it is proved that for undirected Wrapped Butterflies $b(WBF(2, D)) \geq 1.7621D$ ($\approx 1.7621 \log n$) and $b(WBF(3, D)) \geq 2.0002D$ ($\approx 1.2619 \log n$), while for undirected de Bruijn networks $b(DB(2, D)) \geq 1.4404D$ ($= 1.4404 \log n$) and $b(DB(3, D)) \geq 1.8028D$ ($= 1.1374 \log n$).

Concerning lower bounds on gossiping, in the half-duplex mode there is a general lower bound of $1.4404 \log n$ for all graphs of n vertices [5, 15, 14, 19], this bound being attained for complete graphs.

Such lower bound has been generalized in [6], where it has been shown that any s -systolic (i.e. periodic with period s) gossip protocol in the directed and half-duplex modes for any graph takes at least $g(s)(\log n)$ time steps, where $g(s) = 1/(\log 1/\lambda)$ and λ is such that $\sqrt{p_{\lfloor s/2 \rfloor}(\lambda)} \cdot \sqrt{p_{\lceil s/2 \rceil}(\lambda)} = 1$, with $p_j(\lambda) = \lambda + \lambda^3 + \dots + \lambda^{2j-1}$ for any integer $j > 0$. Moreover, improved lower bounds on the gossiping time of s -systolic protocols are provided in the directed, half-duplex and full-duplex cases for Butterfly, de Bruijn and Kautz networks.

Other results concerning specific networks can be found in [4, 12, 7, 11].

In this paper we extend the technique provided in [6] to allow the determination of lower bounds on the broadcasting and gossiping time required by the so-called “restricted” protocols. Informally, a protocol has input restriction i at a given processor if the items delivered during any outgoing activation have been communicated to the processor during at most i of the previous incoming activations. Similarly, the protocol has output restriction o at the processor if the items received during any incoming activation will be delivered by the processor using at most o successive outgoing activations. A protocol with input restriction i and output restriction o is called (i, o) -restricted. For instance, the broadcast protocols running on d -bounded degree networks are $(1, d)$ -restricted, the gossip protocols on d -bounded degree networks (∞, d) -restricted and the s -systolic gossip protocols (i, o) -restricted with $i + o = s$.

We derive the first general lower bounds on the broadcasting and gossiping time of restricted protocols. In particular, every (i, o) -restricted protocol for broadcasting or gossiping in the full-duplex mode takes at least $b(i, o) \log n$ time steps, where $b(i, o) = 1/\log 1/\lambda$ and λ is the solution of $p_o(\lambda) = 1$, with $p_j(\lambda) = \lambda + \lambda^2 + \dots + \lambda^j$ for any integer $j > 0$.

Similarly, in the directed and undirected half-duplex cases, every (i, o) -restricted gossip protocol takes at least $g(i, o) \log n$ time steps, where $g(i, o) = 1/(\log 1/\lambda)$ and

λ is the solution of $\sqrt{p_i(\lambda)} \cdot \sqrt{p_o(\lambda)} = 1$, with $p_j(\lambda) = \lambda + \lambda^3 + \dots + \lambda^{2j-1}$ for any integer $j > 0$. For i and o going to infinity, as a simple corollary this yields the general lower bound independently proved in [5, 15, 14, 19] for all graphs and any (unrestricted) gossip protocol.

As a consequence, by exploiting the fact that every protocol for a graph with parameter d (defined as above) is (∞, d) -restricted, we derive the first general lower bound in the directed and half-duplex modes on the gossiping time of networks with fixed parameter d . This gives 1.5728 for $d = 2$, 1.4829 for $d = 3$, 1.4555 for $d = 4$ and so forth.

For broadcasting and full-duplex gossiping our results for fixed parameter networks coincide with the lower bounds coming from broadcasting [16, 3]. However, if more information about the network topology is known, new lower bounds can be determined for many relevant interconnection networks, such as Butterfly, Wrapped Butterfly, de Bruijn and Kautz networks.

Similarly, improved lower bounds for specific topologies such as Butterfly, Wrapped Butterfly, de Bruijn and Kautz networks are obtained for directed and half-duplex protocols.

Notice that, since as remarked above s -systolic gossip protocol is (i, o) -restricted with $i + o = s$, as a corollary we obtain the same results in [6].

All the results are extended to other communication models, like the c -port and the postal ones. Here new bounds are obtained also in the systolic case.

Even if in this paper we consider only a limited number of networks, our results have wide applicability and give a general framework allowing the determination of improved lower bounds for other graphs by exploiting very general topological properties.

The paper is organized as follows. In the next section we introduce the notation and necessary definitions. In Section 3 we give some useful facts and properties on protocols, matrices and norms. In Section 4 we give the above mentioned lower bounds on the number of steps needed for broadcasting and full-duplex gossiping. In Section 5 we provide the lower bounds on the gossiping time in the directed and half-duplex cases both for general and specific networks. In Section 6 we extend all the results to the c -port and or postal models and finally, in Section 7, we give some conclusive remarks.

2 Notation and Definitions

Let us first introduce some useful notation and definitions.

We model the network as a digraph $G = (V, A)$ in which vertices represent processors and arcs communication links.

Definition 2.1 *A broadcast (resp. gossip) protocol of length t for $G = (V, A)$ is a sequence $\langle A_1, \dots, A_t \rangle$ of t subsets $A_1, \dots, A_t \subseteq A$ subject to the following conditions:*

1. *each A_i , $1 \leq i \leq t$, is a matching in G (i.e. no two arcs in A_i have a common endpoint),*
2. *for a given root vertex $x \in V$ (resp. for any vertex $x \in V$) and for any other vertex $y \in V$, there exists an “informing” path $P(x, y) = \langle x_0, x_1, \dots, x_l \rangle$ with $l \leq t$, $x_0 = x$ and $x_l = y$, and a sequence of positive integers j_1, \dots, j_l such that $1 \leq j_1 < \dots < j_l \leq t$ and for every i , $1 \leq i \leq l$, (x_{i-1}, x_i) belongs to A_{j_i} .*

Informally, each A_i represents the set of arcs which are active at the communication round i . If an arc (x, y) is active at a step i , then at the beginning of step $i + 1$ vertex y knows all the items known by x at the beginning of step i . Then, in order for the sequence of the subsets A_i to be a broadcast (resp. gossip) procedure, starting from the chosen root x (from any vertex x), for any other vertex y there must exist a direct path from x to y whose arcs are activated in a proper sequence so that at the end of the protocol y knows the item of x . We call such a path the informing path from x to y and denote it as $P(x, y)$.

If we restrict our attention to symmetric digraphs, then the above definition corresponds to half-duplex protocols. In order to obtain the full-duplex case, it is sufficient to weaken the condition on active arcs by saying that at every communication round any two active arcs (x, y) and (x', y') are such that either $\{x, y\} \cap \{x', y'\} = \emptyset$ or $x = y'$ and $y = x'$, that is either they don't have a common endpoint or they are opposite. Clearly such a distinction is meaningless for broadcasting, as there is always a single item traveling around and it traverses each link only once and in one direction.

We call (x, y, i) an activation of (x, y) during round i , i.e. when $(x, y) \in A_i$, and we denote as $Act(\langle A_1, \dots, A_t \rangle)$ or simply Act the set of activations of the protocol, i.e. $Act = \{(x, y, i) \mid (x, y) \in A_i, 1 \leq i \leq t\}$. Then we can see an informing path $P(x, y)$ of the protocol from x to y as constituted by the ordered sequence of its activations, i.e. $P(x, y) = \langle (x_0, x_1, j_1), (x_1, x_2, j_2), \dots, (x_{l-1}, x_l, j_l) \rangle$ with $x_0 = x$, $x_l = y$ and $1 \leq j_1 < \dots < j_l \leq t$.

Let $\mathcal{P}(\langle A_1, \dots, A_t \rangle)$ or simply \mathcal{P} be the set of all the information paths of the protocol. Then the protocol performs a broadcasting from a given root $x \in V$ if \mathcal{P}

contains at least an informing path from x to any other vertex $y \in V$. Similarly, for gossiping there must be at least one path for any possible pair of vertices $x, y \in V$.

Given any activation $(x, y, i) \in Act$ incoming at a vertex $y \in V$, in some cases not all the successive outgoing activations (y, z, j) from y depend on (x, y, i) , i.e. carry items that have been communicated to y through (x, y, i) . It is then possible to define a dependence function $D : Act \rightarrow 2^{Act}$ such that, for any $(x, y, i) \in Act$, $D(x, y, i) \subseteq \{(y, z, j) \mid j - i\}$ is the subset of the successive activations outgoing from y that depend on (x, y, i) .

Starting from D , let $\mathcal{P}_D \subseteq \mathcal{P}$ the set of informing paths in \mathcal{P} that respect D , i.e. such that if $\langle (x_0, x_1, j_1), (x_1, x_2, j_2), \dots, (x_{l-1}, x_l, j_l) \rangle \in \mathcal{P}_D$ then for any h , $1 \leq h < l$, $(x_h, x_{h+1}, j_{h+1}) \in D(x_{h-1}, x_h, j_h)$.

Definition 2.2 *A dependence function D is feasible for a broadcast (resp. gossip) protocol $\langle A_1, \dots, A_t \rangle$ if given the root $x \in V$ (resp. for any vertex $x \in V$), given any other vertex $y \in V$, there exists at least an informing path $P(x, y)$ from x to y in \mathcal{P}_D .*

Hence, D is feasible if respecting its dependence relationships does not increase the broadcasting (resp. gossiping) time.

Definition 2.3 *A broadcast (resp. gossip) protocol $\langle A_1, \dots, A_t \rangle$ is (i, o) -restricted at a given vertex $y \in V$ if it admits a feasible dependence function D that satisfies the following two conditions:*

1. *for any outgoing activation $(y, z, j) \in Act$ from y $|\{(x, y, i) \mid (y, z, j) \in D(x, y, i)\}| \leq i$;*
2. *for any incoming activation $(x, y, i) \in Act$ in y $|\{(y, z, j) \mid (y, z, i) \in D(x, y, i)\}| \leq o$.*

Informally, if the protocol is (i, o) -restricted, then every outgoing activation depends on at most i previous incoming activations and every incoming activation influences at most i successive outgoing activations.

In order to prove the lower bounds, we now introduce the notion of *delay digraph* of a restricted protocol.

Definition 2.4 *A delay digraph $DG(A_1 \dots, A_t)$, or simply DG , of a (i, o) -restricted protocol $\langle A_1, \dots, A_t \rangle$ for G is a weighted digraph $DG = (Act, A')$ with $A' = \{((x, y, i), (y, z, j)) \mid (x, y, i) \in Act, (y, z, j) \in Act, (y, z, j) \in D(x, y, i)\}$ and weight function $\delta((x, y, i), (y, z, j)) = j - i$.*

In DG , given two activations $(x, y, i) \in Act$ and $(y, z, j) \in Act$, $\delta((x, y, i), (y, z, j)) = j - i$ is the delay encountered by an item passing (x, y) at time i to cross (y, z) at time j , and according to the dependence function D , delays are represented only between dependent activations.

Definition 2.5 *Given a weighted digraph $G = (V, A)$ with weight function $\delta : A \rightarrow \mathbb{N}^+$ and a positive real number $\lambda \leq 1$, we denote as $M^G(\lambda)$ the $|V| \times |V|$ matrix such that $M^G(\lambda)_{x,y} = \lambda^{\delta(x,y)}$ if $(x, y) \in A$, else $M^G(\lambda)_{x,y} = 0$.*

The key property of the matrix $M^G(\lambda)$ is that, for any positive integer t , $(M^G(\lambda))_{x,y}^t = \sum_{i=1}^m \lambda^{l_i}$, where m is the number of dipaths of t arcs from x to y in G and l_1, \dots, l_m their respective lengths. Then, if $x \neq y$ and there exists a dipath of length at most l from x to y having no more than t arcs, as $0 \leq \lambda \leq 1$ it is $\sum_{i=1}^t (M^G(\lambda))_{x,y}^i \geq \lambda^l$.

The matrix $M^{DG}(\lambda)$ is called the *delay matrix* of G with respect to the (i, o) -restricted protocol and is denoted simply as $M(\lambda)$.

3 Preliminaries

In this section we introduce some basic properties and facts that will be used in the following sections.

First of all, let us give some examples of (i, o) -restricted protocols. The first one concerns bounded degree networks. In fact, let the parameter d be defined for undirected graphs as the maximum degree minus one and for directed graphs as the maximum out-degree. Then the following lemma holds.

Lemma 3.1 *Every protocol for a network with fixed parameter d at each vertex is (∞, d) -restricted.*

Proof. The claim derives by observing that an item of information needs to traverse a given arc only once. Since at any vertex $y \in V$ for every activation (x, y, i) there are at most d successive activations of the type (y, z, j) , $j > i$, corresponding to different arcs, then it is possible to put in the dependence set $D(x, y, i)$ the at most d elements obtained by the first activation of the any arc leaving y (clearly except (y, x)), maintaining in \mathcal{P}_D at least one informing path between each pair of vertices having an informing path in \mathcal{P} . \square

Another example is constituted by the s -systolic protocols, i.e. with $A_i = A_{i+s}$ for each $1 \leq i \leq t - s$.

Lemma 3.2 *Every s -systolic protocol at each vertex is (i, o) -restricted with $i + o \leq s$.*

Proof. Given a vertex y , let l and r be respectively the number of incoming and outgoing activations during a systolic period. Since a period contains s activations, then $l + r \leq s$. Analogously as in the previous lemma, since for any activation (x, y, i) there are at most r successive activations of the type (y, z, j) , $j > i$, corresponding to different arcs, then it is possible to put in the dependence set $D(x, y, i)$ the r outgoing activations that are within the next systolic period. This maintains in \mathcal{P}_D at least one informing path between each pair of vertices having an informing path in \mathcal{P} . The lemma follows by observing that $o = r$ and that by construction each outgoing activation belongs to the dependence set of the l incoming activations belonging to the previous systolic period. Hence $i = l$ and $i + o = l + r = s$. \square

Notice that in bounded degree networks it is not possible to bound the input restriction. In fact, if there are different activations of an incoming arc, then any successive outgoing activation might depend on all the incoming activations, because each might carry different items. Even if this is true also for systolic protocols, by the periodic fashion if we bound the input restriction as shown in the previous lemma, this guarantees that the proper information paths are maintained, and are all the ones in which any two successive activations along each path are distant at most s steps. Notice also that in case of broadcasting the input restriction i is equal to 1, since for each vertex $y \in V$ there is only one incoming activation $(x, y, i) \in Act$. In fact, if there is more than one, it is possible to maintain in Act only the first one without increasing the broadcasting time.

As we will see in the following sections, better lower bounds can be determined when some information about the topology of the network is known. More precisely, this is possible if the network contains a large number of faraway vertices.

Definition 3.1 *Given two positive real numbers α and l , a digraph $G = (V, A)$ has an $\langle \alpha, l \rangle$ -broadcast separator if there exist a root vertex x and a subset of vertices $V_x \subset V$ such that $\min_{y \in V_x} \text{dist}_G(x, y) = l(\log n)(1 - o(1))$ and $|V_x| \geq 2^{\alpha l(\log n)(1 - o(1))}$.*

An analogous definition can be given for gossiping.

Definition 3.2 *Given two positive real numbers α and l , a digraph $G = (V, A)$ has an $\langle \alpha, l \rangle$ -gossip separator if there exist two subsets of vertices $V_1 \subset V$ and $V_2 \subset V$ such that $\min_{x \in V_1, y \in V_2} \text{dist}_G(x, y) = l(\log n)(1 - o(1))$ and $\min(|V_1|, |V_2|) \geq 2^{\alpha l(\log n)(1 - o(1))}$.*

Notice that by definition $\alpha \cdot l \leq 1$. Moreover, an $\langle \alpha, l \rangle$ -gossip separator for G implies the existence of an $\langle \alpha, l \rangle$ -broadcast separator.

Many well-known interconnection networks admit good separators, like for instance Butterfly, de Bruijn and Kautz graphs.

Lemma 3.3 [6]

There exists an $\langle \alpha, l \rangle$ -separator with

1. $\alpha = (\log d)/2$ and $l = 2/(\log d)$ for Unwrapped Butterflies $BF(d, D)$ of degree d and dimension D ;
2. $\alpha = (\log d)/2$ and $l = 2/(\log d)$ for directed Wrapped Butterflies $\vec{WBF}(d, D)$;
3. $\alpha = 2(\log d)/3$ and $l = 3/(2 \log d)$ for undirected Wrapped Butterflies $WBF(d, D)$;
4. $\alpha = \log d$ and $l = 1/\log d$ for undirected de-Bruijn networks $DB(d, D)$;
5. $\alpha = \log d$ and $l = 1/\log d$ for undirected Kautz networks $K(d, D)$.

We conclude the section by recalling some useful definitions and properties about matrices that are well-known in linear algebra (see for instance [1, 6]).

Let \mathcal{R}^m be the set of all column vectors of m real elements. A real function $|| \cdot || : \mathcal{R}^m \rightarrow \mathcal{R}$ is called a *norm* if $|X| \geq 0$ for every $X \in \mathcal{R}^m$, $|X| = 0$ if and only if all the m components of X are equal to 0, $|aX| = \text{abs}(a)|X|$ for every $a \in \mathcal{R}$ and $X \in \mathcal{R}^m$ ($\text{abs}(a)$ being the absolute value of a), and finally $|X + Y| \leq |X| + |Y|$ for all $X, Y \in \mathcal{R}^m$.

For any integer $d > 0$, the d -norm of a vector $X \in \mathcal{R}^m$ is defined as $|X|_d = \left(\sum_{j=1}^m \text{abs}(x_j)^d \right)^{1/d}$. The d -norm $||M||_d$ of an $n \times m$ real matrix M is $\sup_{X \in \mathcal{R}^m, |X|_d \neq 0} \frac{|MX|_d}{|X|_d}$. $|X|_2$ and $||M||_2$ are the Euclidean vector and matrix norms, respectively, while $|X|_\infty = \max_{j=1}^m \text{abs}(x_j)$ and $||M||_\infty = \max_{i=1}^n \left(\sum_{j=1}^m \text{abs}(m_{i,j}) \right)$ are called vector and matrix maximum norms.

For every matrix M with non negative real elements, the Euclidean matrix norm satisfies the following properties:

1. $||M||_d \geq 0$;
2. $||M||_d = 0 \Rightarrow M = 0$;
3. $\forall a \in \mathcal{R}, ||aM||_d = \text{abs}(a)||M||_d$;

4. $M \geq N \Rightarrow \|M\|_d \geq \|N\|_d$;
5. $\|M + N\|_d \leq \|M\|_d + \|N\|_d$;
6. $\|MN\|_d \leq \|M\|_d \cdot \|N\|_d$;
7. if N is obtained from M by row and column permutations, $\|N\|_d = \|M\|_d$;
8. if M is everywhere null except in k subblocks M_1, \dots, M_k not sharing any row or column, then $\|M\|_d = \max_{i=1}^k \|M_i\|_d$.

Definition 3.3 *Given an $m \times m$ real matrix M , a non null column vector $X \in \mathcal{R}^m$ is an eigenvector for M with eigenvalue e if $MX = eX$. The spectral radius $\rho(M)$ of M is the maximum absolute value of an eigenvalue of M .*

The spectral radius of a matrix M is related to the Euclidean norm of M . In fact, $\|M\|_2 = \sqrt{\rho(M^T \cdot M)}$, where M^T is the transpose of M , and if M is symmetric $\|M\|_2 = \rho(M)$. Moreover, for any natural matrix norm, that is defined from any vector norm $|X|'$ as $\sup_{X \in \mathcal{R}^m, |X|' \neq 0} \frac{|MX|'}{|X|'}$, $\|M\|' \geq \rho(M)$.

Given an $m \times m$ matrix M , a non null column vector $X \in \mathcal{R}^m$ is a *semi-eigenvector* for M with *semi-eigenvalue* e if $MX \leq eX$.

Lemma 3.4 [6]

Given an $m \times m$ non negative matrix M and a strictly positive semi-eigenvector $X \in \mathcal{R}^m$ of M with semi-eigenvalue e , $\rho(M) \leq e$.

4 Lower Bounds for Broadcasting

In this section we provide new lower bounds on the broadcasting time of the (i, o) -restricted protocols. As already remarked, without loss of generality we can assume that $i = 1$, since there is only one incoming activation at each vertex. Moreover, we implicitly assume $o > 1$, otherwise each vertex except the root can inform at most another vertex. This means that at each step at most two new vertices can know the item of the root, thus yielding at least $n/2$ steps, where n is the total number of vertices.

In this section, for the sake of brevity, $| \cdot |$ and $\| \cdot \|$ will denote the vector and matrix norms of the maximum, i.e. $| \cdot | = | \cdot |_\infty$ and $\| \cdot \| = \| \cdot \|_\infty$.

Theorem 4.1 *Let $\langle A_1, \dots, A_t \rangle$ be a $(1, o)$ -restricted broadcast protocol for a digraph $G = (V, A)$, $o > 1$. Then $t \geq b(1, o)(\log n) - O(\log \log n)$, where $n = |V|$, $b(i, o) = \frac{1}{(\log 1/\lambda)^i}$ and λ is any positive real number such that $p_o(\lambda) \leq 1$, with $p_o(\lambda) = \lambda + \lambda^2 + \dots + \lambda^o$.*

Proof. Consider the delay digraph $DG = (Act, A')'$ and let $m = |Act| \leq tn/2$ (every node in G can have at most t activated incident arcs, one per round). By the properties of $M(\lambda)$, if x is the root vertex of the protocol, there exists an $m \times m$ boolean matrix N satisfying the following conditions:

- for any vertex $z \in V$ of G with $x \neq y$, there exist exactly two vertices $(x, y, i) \in Act$ and $(w, z, j) \in Act$ such that the corresponding element of N in the row of (x, y, i) and column of (w, z, j) is equal to 1;
- $M(\lambda) + M(\lambda)^2 + \dots + M(\lambda)^t \geq \lambda^t N$.

The above conditions state that for any non root vertex z of G there must exist two activations $(x, y, i) \in Act$ and $(w, z, j) \in Act$ whose distance in DG is at most t , i.e. such that the item of x , starting from the communication round i in which it traverses (x, y) , steps through arc (w, z) after at most t rounds. Clearly, since all weights in DG are at least equal to 1, any dipath in DG from (x, y, i) to (w, z, j) of length at most t is constituted by at most t arcs.

By the norm properties,

$$\|M(\lambda) + M(\lambda)^2 + \dots + M(\lambda)^t\| \geq \|\lambda^t N\| = \lambda^t \|N\|,$$

therefore

$$\begin{aligned} \|M(\lambda)\| + \|M(\lambda)\|^2 + \dots + \|M(\lambda)\|^t &\geq \|M(\lambda)\| + \|M(\lambda)^2\| + \dots + \|M(\lambda)^t\| \geq \\ &\|M(\lambda) + M(\lambda)^2 + \dots + M(\lambda)^t\| \geq \lambda^t \|N\|. \end{aligned}$$

But

$$\|M(\lambda)\| = \max_{i=1}^t \sum_{j=1}^m m_{i,j} \leq \lambda^{i_1} + \lambda^{i_2} + \dots + \lambda^{i_o} \leq p_o(\lambda),$$

as there are at most o entries different from 0 in each row of M , each corresponding to a different power of λ . In fact, each row is associated to an activation (y, z, i) incoming at z , while the at most o entries (z, w, j) in the row that are different from

0 correspond to the successive activations outgoing from z that are influenced by (y, z, i) , each at a different round j .

Moreover,

$$\|N\| = \max_{i=1}^m \sum_{j=1}^m n_{i,j} \geq \frac{(n-1)}{t},$$

since there are $(n-1)$ entries equal to 1 in N , distributed on the most t rows corresponding to the activations (x, y, i) outgoing from the root.

By the choice of λ , $\|M(\lambda)\| \leq p_o(\lambda) \leq 1$, and

$$t \geq \|M(\lambda)\| + \|M(\lambda)\|^2 + \dots + \|M(\lambda)\|^t \geq \lambda^t \|N\|,$$

$$\text{that is } t \geq \frac{(\log \|N\|) - (\log t)}{(\log 1/\lambda)} \geq \frac{(\log n - 1) - 2(\log t)}{(\log 1/\lambda)}.$$

The claim then follows by observing that if $t = \omega(\log n)$ the above inequality trivially holds, while if $t = O(\log n)$ then $2(\log t) = O(\log \log n)$. \square

As an application of the previous theorem and of Lemma 3.1, general lower bounds can be obtained for bounded degree networks that coincide with the ones provided in [16, 3]. However, if more information about the separating properties of the network is known, by refining the above theorem tighter bounds can be determined.

Theorem 4.2 *Let $\langle A_1, \dots, A_t \rangle$ be an $(1, o)$ -restricted gossip broadcast protocol for a digraph $G = (V, A)$ with an $\langle \alpha, l \rangle$ -broadcast separator. Then $t \geq b(1, o)(\log n)(1 - o(1))$, where $b(1, o) = \max_{\lambda \mid p_o(\lambda) \leq 1} l \left(\frac{\alpha - (\log p_o(\lambda))}{(\log 1/\lambda)} \right)$ and $p_o(\lambda) = \lambda + \lambda^2 + \dots + \lambda^o$.*

Proof. Consider the delay digraph $DG = (Act, A')$ and let $m = |Act| \leq tn/2$. Moreover, let $d = \min_{y \in V_x} \text{dist}_G(x, y)$ and $c = |V_x|$, where x and Act are the root vertex and the set associated to the $\langle \alpha, l \rangle$ -broadcast separator of G .

Similarly as in the proof of Theorem 4.1, there exists an $m \times m$ boolean matrix N satisfying the following conditions:

- for any vertex $z \in V_x$ of G , there exist exactly two vertices $(x, y, i) \in Act$ and $(w, z, j) \in Act$ such that the corresponding element of N in the row of (x, y, i) and column of (w, z, j) is equal 1; all the other elements are null;
- $M(\lambda)^{d-1} + \dots + M(\lambda)^t \geq \lambda^t N$.

The above conditions state that for any vertex $z \in V_x$ of G , there must exist two activations $(x, y, i) \in Act$ and $(w, z, j) \in Act$ whose distance in DG is at most t . Moreover, as x and z are at distance at least d in G , any dipath in DG from (x, y, i) to (w, z, j) contains at least $d - 1$ different arcs.

By the norm properties,

$$\|M(\lambda)^{d-1} + \dots + M(\lambda)^t\| \geq \|\lambda^t N\| = \lambda^t \|N\|.$$

Again, $\|M(\lambda)\| \leq p_o(\lambda)$, and $\|N\| = \max_{i=1}^t \sum_{j=1}^m n_{i,j} \geq \frac{c}{t}$, since there are c entries equal 1 in N , distributed on the at most t rows corresponding to the activations (x, y, i) outgoing from the root.

Therefore,

$$\|M(\lambda)\|^{d-1} + \|M(\lambda)\|^{d-2} + \dots + \|M(\lambda)\|^t \geq \|M(\lambda)^{d-1}\| + \|M(\lambda)^{d-2}\| + \dots + \|M(\lambda)^t\| \geq$$

$$\|M(\lambda)^{d-1} + M(\lambda)^{d-2} + \dots + M(\lambda)^t\| \geq \lambda^t \frac{c}{t}.$$

Finally, for every λ such that $p_o(\lambda) \leq 1$, $\|M(\lambda)\| \leq p_o(\lambda) \leq 1$, and

$$(t - d + 2)\|M(\lambda)\|^{d-1} \geq \lambda^t c/t,$$

that is

$$t \geq \frac{(\log c) - (d - 1)(\log \|M(\lambda)\|) - (\log t - d + 2) - (\log t)}{(\log 1/\lambda)} \geq$$

$$\frac{\alpha l(\log n) - l(\log n)(\log \|M(\lambda)\|) - o(l \log n) - (\log t - d + 2) - (\log t)}{(\log 1/\lambda)} \geq$$

$$l \left(\frac{\alpha - (\log p_o(\lambda))}{(\log 1/\lambda)} \right) (\log n)(1 - o(1)).$$

In fact, if $t = \omega(l \log n)$ the above inequality trivially holds, while if $t = O(l \log n)$ it derives directly by observing that $(\log t - d + 2) + (\log t) = O(\log t) = O((\log l \log n))$. \square

By applying Theorem 4.2 and Lemma 3.3, the following lower bounds for Butterfly, de Bruijn and Kautz networks can be determined.

Corollary 4.3 *The lower bounds on the broadcasting time for $BF(d, D)$, $W\vec{B}F(d, D)$, $WBF(d, D)$, $DB(d, D)$ and $K(d, D)$ in Figure 1 hold.*

	ours	previous
$b(BF(2, D))$	2.2104	2 (diam.)
$b(BF(3, D))$	1.5203	1.2618 (diam.)
$b(BF(4, D))$	1.2938	1.0058 [16, 3]
$b(BF(5, D))$	1.1837	1.0014 [16, 3]
$b(W\vec{B}F(2, D))$	2.2200	1.7621 [18]
$b(W\vec{B}F(3, D))$	1.5244	1.2619 [18]
$b(W\vec{B}F(4, D))$	1.2957	1.0058 [16, 3]
$b(W\vec{B}F(5, D))$	1.1847	1.0014 [16, 3]
$b(WBF(4, D))$	1.1047	1.0058 [16, 3]
$b(WBF(5, D))$	1.0433	1.0014 [16, 3]
$b(K(2, D))$	1.3042	1.1374 [16, 3]
$b(K(3, D))$	1.0433	1.0254 [16, 3]

Figure 1: Some lower bounds for broadcasting. $t \geq b(G)(\log n)(1 - o(1))$. The unlisted cases coincide with those in [16, 3], except for Wrapped Butterflies and de-Bruijn with $d = 2, 3$ for which better bounds are given in [18]. “diam.” stands for diameter.

Notice that in the above corollary we have made use of gossip separators since broadcast separators can not yield better values of α and l . In fact, in all the cases $\alpha \cdot l = 1$ and $l \cdot \log n$ coincides with the diameter up to a negligible additive factor.

5 Lower Bounds for Gossiping

In this section we provide lower bounds on the gossiping time of the (i, o) -restricted gossip protocols. We consider only the directed and half-duplex cases, since in the full-duplex mode the results coincide with those for broadcasting. We give both lower bounds holding for any network and refined ones that exploit the separating properties.

As an application, new lower bounds can be determined for bounded degree networks, both for general and specific topologies.

For the sake of brevity, in this section $||$ and $|||$ will denote the Euclidean vector and matrix norms, i.e. $||| = ||_2$ and $||| = |||_2$.

Similarly as for broadcasting, the following lemmas hold.

Lemma 5.1 [6]

Let $\langle A_1, \dots, A_t \rangle$ be an (i, o) -restricted gossip protocol for a digraph $G = (V, A)$, $s > 2$. Then $t \geq g(i, o)(\log n) - O(\log \log n)$, where $n = |V|$, $g(i, o) = \frac{1}{(\log 1/\lambda)}$ and λ is any real number such that $0 \leq \lambda \leq 1$ and $\|M(\lambda)\| \leq 1$.

The following lemma can be used for digraphs admitting good separators.

Lemma 5.2 [6]

Let $\langle A_1, \dots, A_t \rangle$ be an (i, o) -restricted gossip protocol for a digraph $G = (V, A)$ with an $\langle \alpha, l \rangle$ -separator. Then $t \geq g(i, o)(\log n)(1 - o(1))$, where

$$g(i, o) = \max_{\lambda \mid \|M(\lambda)\| \leq 1} l \left(\frac{\alpha - (\log \|M(\lambda)\|)}{(\log 1/\lambda)} \right).$$

As a direct consequence of Lemma 5.1 and 5.2, the problem of deriving lower bounds on the gossiping time is reduced to the determination of the norm of the matrix $M(\lambda)$ associated to (i, o) -restricted gossip protocols. While this task is more and less trivial in broadcasting with the norm of the maximum (this is why we incorporated it directly in the proof), it is more difficult for the Euclidean norm. We now show how this can be accomplished by means of successive simplification steps performed on $M(\lambda)$.

Observe first that, by the properties of the matrix norm, the value of $\|M(\lambda)\|$ is not affected by any row or column permutation of $M(\lambda)$. By the definition of DG , for every vertex x of the initial graph G , all vertices (y, x, i) in DG can be connected only to vertices (x, z, j) in DG and to no other vertex of DG . It is then possible to permute the rows of $M(\lambda)$ in such a way that for every x all vertices (y, x, j) in DG correspond to adjacent rows and all vertices (x, z, j) to adjacent columns. The resulting matrix is everywhere null, except in disjoint subblocks $M_1(\lambda), \dots, M_n(\lambda)$ such that for any $i \neq j$ blocks $M_i(\lambda)$ and $M_j(\lambda)$ have not any common row or column. Informally, each subblock $M_i(\lambda)$ corresponds as above to a vertex x of the initial graph G and reports the delays between its incoming and its outgoing activations.

By the properties of the matrix norm $\|M(\lambda)\| = \max_i \|M_i(\lambda)\|$, hence in the remaining part of this section we concentrate on the determination of each $\|M_i(\lambda)\|$.

As already observed, each $M_i(\lambda)$ expresses the local protocol occurring around a fixed vertex x in G . Every row of $M_i(\lambda)$ corresponds to an incoming activation of x , that is to a vertex (y, x, j) in the delay graph DG , and every column corresponds to an outgoing activation of x , that is to a vertex (x, y, j) of DG .

We implicitly assume that at each round an arc incident to x is activated. In fact, any local matrix not satisfying this property can be obtained from one in which the property is satisfied (which corresponds to a complete local protocol at vertex x) by deleting the rows corresponding to the removed incoming activations and the columns corresponding to the removed outgoing activations. This can not increase $\|M_i(\lambda)\|$ and, since in order to apply Lemma 5.1 and 5.2 we are interested in determining upper bounds for $\|M_i(\lambda)\|$, it does not affect the correctness of our proof. Moreover, we assume that the protocol locally at x starts with an incoming activation and ends with an outgoing activation, since this corresponds to delete initial columns of 0s and final rows of 0s in $M_i(\lambda)$, again without affecting its norm.

In order to describe the properties of $M_i(\lambda)$, we first point out that a protocol locally at the vertex x is characterized by two sequences of positive integers $\langle (l_j)_{j=\{1\dots k\}}, (r_j)_{j=\{1\dots k\}} \rangle$. In fact, starting from the first incoming activation at round 1, the protocol locally at x has l_1 successive incoming activations (from round 1 to round l_1), then r_1 successive outgoing activations, then again l_2 incoming activations and r_2 outgoing activations, and so on until the last l_k incoming activations and r_k outgoing activations, where k is a suitable positive integer such that $k \leq \lfloor t/2 \rfloor$. Clearly $\sum_{j=1}^k l_j + r_j \leq t$.

Definition 5.1 *Given the couple of sequences $\langle (l_j)_{j=\{1\dots k\}}, (r_j)_{j=\{1\dots k\}} \rangle$ associated with the local protocol at vertex x , the incoming (resp. outgoing) activation block j is the set of the successive incoming (resp. outgoing) activations corresponding to l_j (resp. r_j).*

Hence for instance the incoming activation block 1 corresponds to the first l_1 incoming activations, block 2 to the next l_2 incoming activations, ..., and block k to the last l_k activations.

Since permuting the rows and columns of $M_i(\lambda)$ does not affect $\|M_i(\lambda)\|$, we can assume the following ordering of the rows and columns of $M_i(\lambda)$:

- rows occur in order of incoming activation block and inside each block in reverse order of round. So for instance the first row corresponds to the l_1 -th incoming activation of block 1 and row l_1 to the first one;
- columns occur in order of outgoing activation block and inside each block this time in order of round. Hence column 1 is associated to the first outgoing activation of block 1 and column r_1 to the last one.

By construction, $M_i(\lambda)$ can be divided in k^2 blocks $B_{1,1}, \dots, B_{k,k}$ such that $B_{h,j}$ corresponds to the incoming activation block h and the outgoing activation block j

λ	λ^2	λ^4	λ^5	λ^8	λ^9	λ^{10}	λ^{14}	...
λ^2	λ^3	λ^5	λ^6	λ^9	λ^{10}	λ^{11}	λ^{15}	...
0	0	λ	λ^2	λ^5	λ^6	λ^7	λ^{11}	...
0	0	0	0	λ	λ^2	λ^3	λ^7	...
0	0	0	0	λ^2	λ^3	λ^4	λ^8	...
0	0	0	0	0	0	0	λ	...
0	0	0	0	0	0	0	λ^2	...
0	0	0	0	0	0	0	λ^3	...
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	

λ	0	λ^4	0	λ^8	λ^9	0	0	...
0	λ^3	λ^5	0	λ^9	0	λ^{11}	0	...
0	0	λ	λ^2	0	λ^6	λ^7	0	...
0	0	0	0	λ	0	λ^3	0	...
0	0	0	0	0	λ^3	0	λ^8	...
0	0	0	0	0	0	0	λ	...
0	0	0	0	0	0	0	0	...
0	0	0	0	0	0	0	λ^3	...
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	

Figure 2: Two examples of $M_i(\lambda)$ with $l_1 = 2$, $r_1 = 2$, $l_2 = 1$, $r_2 = 2$, $l_3 = 2$, $r_3 = 3$, $l_4 = 3$, $r_4 = 1$, ..., where we have emphasized blocks $B_{i,j}$ with $1 \leq i, j \leq 4$. The first matrix correspond to an unrestricted protocol, while the second to a $(3, 4)$ -restricted one (at most 4 non null entries per row and 3 per column).

and is given by the intersection of the associated rows and columns (see Figure 2). If $j < h$ then $B_{h,j}$ has all entries equal to 0, since each incoming activation in block h influences only the successive outgoing activations, i.e. in the outgoing activation blocks from h to k . Moreover, in each block $B_{h,j}$ with $j \geq h$ any entry is different from 0 if the incoming activation associated to its row influences the outgoing activation associated to its column, according to the dependence function D . In fact, only such delays are represented in the delay graph. Two examples of $M_i(\lambda)$ can be found in Figure 2.

The following vectors and matrix operations can be used to suitably express $M_i(\lambda)$ and its semi-eigenvectors.

- Λ_j is the column vector whose components are $1, \lambda, \dots, \lambda^{j-1}$;

1	0	1	0	1	1	0	0	...
0	1	1	0	1	0	1	0	...
0	0	1	1	0	1	1	0	...
0	0	0	0	1	0	1	0	...
0	0	0	0	0	1	0	1	...
0	0	0	0	0	0	0	1	...
0	0	0	0	0	0	0	0	...
0	0	0	0	0	0	0	1	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Figure 3: The restriction matrix D_i associated to the $(3, 4)$ -restricted protocol of Figure 2 (at most 4 entries equal to 1 per row and 3 per column).

- given two column vectors X and Y respectively of h and j components, $X \searrow Y$ is the vertical concatenation of X and Y , i.e. the column vector of $h + j$ components such that the first h components coincide with the ones of X and the last remaining j components coincide with the ones of Y ;
- given a column vector X , X^T is the row vector obtained by transposing X ;
- given two $a \times b$ matrices A and B , $A \otimes B$ is the componentwise product operation of A and B , i.e. the matrix whose element at row h and column j is $a_{h,j} \cdot b_{h,j}$.

By construction $M_i(\lambda)$ can be expressed as the componentwise product $D_i \otimes N_i(\lambda)$ of two matrices D_i and $N_i(\lambda)$ constructed as follows.

D_i is a boolean matrix in which each element is equal to 1 if and only if the corresponding element in $M_i(\lambda)$ is non null, that is if the outgoing activation associated to its column belongs to the dependence set of the incoming activation associated to its row. Since the protocol is (i, o) -restricted, then there are at most o elements equal to 1 in each row and at most i in each column (see Figure 3).

$N_i(\lambda)$ can be seen as the local matrix around vertex x in which there is no input-output restriction, that is every incoming activation influences all the successive outgoing activations (like for instance the first matrix of Figure 2).

For any integer j , $0 \leq j \leq k$, let sl_j and sr_j be defined as $\sum_{g=1}^{j-1} l_g$ and $\sum_{g=1}^{j-1} r_g$, respectively (hence $sl_0 = sr_0 = 0$). Then $B_{h,j}$ is given by the intersection of rows from $sl_{h-1} + 1$ to sl_h and columns from $sr_{j-1} + 1$ to sr_j . Moreover, if $h \leq j$, given any two integers a and b such that $sl_{h-1} + 1 \leq a \leq sl_h$ and $sr_{j-1} + 1 \leq b \leq sr_j$,

$$\begin{array}{ccccccc}
& & \vdots & & \vdots & & \vdots \\
\cdots & d_{sl_{h-1}+1, sr_{j-1}+1} \lambda^{\delta_{h,j}} & & d_{sl_{h-1}+1, sr_{j-1}+2} \lambda^{\delta_{h,j}+1} & \cdots & d_{sl_{h-1}+1, sr_j} \lambda^{\delta_{h,j}+r_j-1} & \cdots \\
\cdots & d_{sl_{h-1}+2, sr_{j-1}+1} \lambda^{\delta_{h,j}+1} & & d_{sl_{h-1}+2, sr_{j-1}+2} \lambda^{\delta_{h,j}+2} & \cdots & d_{sl_{h-1}+2, sr_j} \lambda^{\delta_{h,j}+r_j} & \cdots \\
& & \vdots & & \vdots & & \vdots \\
\cdots & d_{sl_h, sr_{j-1}+1} \lambda^{\delta_{h,j}+l_h-1} & & d_{sl_h, sr_{j-1}+2} \lambda^{\delta_{h,j}+l_h} & \cdots & d_{sl_h, sr_j} \lambda^{\delta_{h,j}+l_h+r_j-2} & \cdots \\
& & \vdots & & \vdots & & \vdots
\end{array}$$

Figure 4: Block $B_{h,j}$ in $M_i(\lambda)$.

the element of $M_i(\lambda)$ at row a and column b (hence belonging to $B_{h,j}$) is equal to $d_{a,b} \lambda^{\delta_{h,j}} \lambda^{a-sl_{h-1}-1} \lambda^{b-sr_{j-1}-1}$, where $\delta_{h,j}$ is the number of rounds between the last activation of the incoming activation block h and the first activation of the outgoing activation block j , that is $\delta_{h,j} = 1$ if $h = j$, otherwise $\delta_{h,j} = 1 + \sum_{g=h}^{j-1} (r_g + l_{g+1}) = sr_j - sr_{h-1} + sl_{j+1} - sl_h + 1$ (see Figure 4)

In the particular case in which all the $d_{a,b}$ of D_i are equal to 1 in $B_{h,j}$, then $B_{h,j}$ can be suitably expressed as $B_{h,j} = \lambda^{\delta_{h,j}} \Lambda^{l_h} (\Lambda^{r_j})^T$.

Let $\Lambda = (\lambda^{x_1} \cdot \Lambda_{r_1}) \searrow (\lambda^{x_2} \cdot \Lambda_{r_2}) \searrow \cdots \searrow (\lambda^{x_k} \cdot \Lambda_{r_k})$ and $\Theta = (\lambda^{x_1} \cdot \Lambda_{l_1}) \searrow (\lambda^{x_2} \cdot \Lambda_{l_2}) \searrow \cdots \searrow (\lambda^{x_k} \cdot \Lambda_{l_k})$, where $x_h = \sum_{g=1}^{h-1} (r_g - l_{g+1}) = sr_{h-1} - sl_h + sl_1$, $1 \leq h \leq k$ (thus $x_1 = 0$).

The vectors Λ and Θ thus defined have the particular property that if we multiply each column b of $M_i(\lambda)$ by the b -th element of Λ , then any row a contains different odd powers of λ , multiplied times the a -th element of Θ . This means that the sum of all the elements of row a , which is equal to the a -th element of the vector $M_i(\lambda) \cdot \Lambda$, is at most equal to the a -th element of Θ multiplied by $p_o(\lambda)$, as there are at most o non null entries per row (see Figure 5).

Similar considerations hold multiplying the a -th column of $M_i(\lambda)^T$ by the a -th element of Θ , so that the b -th element of $M_i(\lambda) \cdot \Theta$ is at most equal to the b -th element of Λ multiplied by $p_i(\lambda)$.

Therefore it is possible to prove the following lemma.

Lemma 5.3 $\|M(\lambda)\| \leq \sqrt{p_i(\lambda)} \sqrt{p_o(\lambda)}$, where for any even positive integer j , the polynomial $p_j(\lambda) = \lambda + \lambda^3 + \cdots + \lambda^{2j-1}$.

$$\begin{array}{c|c|c}
 \begin{array}{cccccccc}
 \lambda & \lambda^3 & \lambda^5 & \lambda^7 & \lambda^9 & \lambda^{11} & \lambda^{13} & \lambda^{15} & \dots \\
 \lambda^2 & \lambda^4 & \lambda^6 & \lambda^8 & \lambda^{10} & \lambda^{12} & \lambda^{14} & \lambda^{16} & \dots \\
 0 & 0 & \lambda & \lambda^3 & \lambda^5 & \lambda^7 & \lambda^9 & \lambda^{11} & \dots \\
 0 & 0 & 0 & 0 & \lambda & \lambda^3 & \lambda^5 & \lambda^7 & \dots \\
 0 & 0 & 0 & 0 & \lambda^2 & \lambda^4 & \lambda^6 & \lambda^8 & \dots \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda^2 & \dots \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda^3 & \dots \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda^4 & \dots \\
 \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
 \end{array} &
 \Theta = &
 \begin{array}{c}
 1 \\
 \lambda \\
 \lambda \\
 \lambda \\
 \lambda \\
 \lambda^2 \\
 \lambda \\
 \lambda^2 \\
 \lambda^3 \\
 \vdots
 \end{array}
 \end{array}
 \begin{array}{c}
 \leq p_\infty(\lambda) \\
 \leq \lambda p_\infty(\lambda) \\
 \leq \lambda p_\infty(\lambda) \\
 \leq \lambda p_\infty(\lambda) \\
 \leq \lambda^2 p_\infty(\lambda) \\
 \leq \lambda p_\infty(\lambda) \\
 \leq \lambda^2 p_\infty(\lambda) \\
 \leq \lambda^2 p_\infty(\lambda) \\
 \leq \lambda^3 p_\infty(\lambda)
 \end{array}$$

$$\begin{array}{c|c}
 \begin{array}{cccccccc}
 1 & \lambda & \lambda & \lambda^2 & \lambda & \lambda^2 & \lambda^3 & \lambda & \dots
 \end{array} & = \Lambda^T
 \end{array}$$

Figure 5: $M_i(\lambda)$ of the unrestricted protocol of Figure 2, with the vectors Λ (transposed) and Θ , where all entries of column b in $M_i(\lambda)$ have been multiplied by the b -th element of Λ . On the right there is an upper bound on the sum of the elements of each row in the new matrix.

Proof. By Lemma 3.4, it is sufficient to show that Λ is a semi-eigenvector of $M_i(\lambda)^T \cdot M_i(\lambda)$ with semi-eigenvalue $p_i(\lambda)p_o(\lambda)$, so that $\|M(\lambda)\| = \max_i \|M_i(\lambda)\| = \max_i \sqrt{\rho(M_i(\lambda)^T \cdot M_i(\lambda))} \leq \sqrt{p_i(\lambda)} \sqrt{p_o(\lambda)}$.

By definition, if b is any integer such that $sr_{j-1} < b \leq sr_j$ for a suitable $j > 0$, that is column b in M corresponds to the outgoing activation block j , then the b -th element of the semi-eigenvector Λ is equal to $\lambda^{b-sr_{j-1}-1} \cdot \lambda^{sr_{j-1}-sl_j+sl_1} = \lambda^{b-sl_j+sl_1-1}$. Similarly, if a is any integer such that $sl_{j-1} < a \leq sl_j$, that is row a in M corresponds to the incoming activation block j , then the a -th element of vector Θ is equal to $\lambda^{a-sl_{j-1}-1} \cdot \lambda^{sr_{j-1}-sl_j+sl_1}$. Thus, the a -th element of $M \cdot \Lambda$ (i.e. the product of row a of M and Λ) is equal to

$$\begin{aligned}
 & \lambda^{a-sl_{j-1}-1} \left(\sum_{b=sr_{j-1}+1}^{sr_j} d_{a,b} \lambda \lambda^{b-sr_{j-1}-1} \lambda^{b-sl_j+sl_1-1} + \right. \\
 & \sum_{b=sr_j+1}^{sr_{j+1}} d_{a,b} \lambda^{sr_j-sr_{j-1}+sl_{j+1}-sl_j+1} \lambda^{b-sr_j-1} \lambda^{b-sl_{j+1}+sl_1-1} + \dots + \\
 & \left. \sum_{b=sr_{k-1}+1}^{sr_k} d_{a,b} \lambda^{sr_{k-1}-sr_{j-1}+sl_k-sl_j+1} \lambda^{a-sr_{k-1}-1} \lambda^{b-sl_k+sl_1-1} \right) =
 \end{aligned}$$

$$\begin{aligned}
& \lambda^{a-sl_{j-1}} \cdot \lambda^{sr_{j-1}-sl_j+sl_1-1} \left(\sum_{b=sr_{j-1}+1}^{sr_j} d_{a,b} \lambda^{b-sr_{j-1}-1} \lambda^{b-sr_{j-1}+} \right. \\
& \sum_{b=sr_j+1}^{sr_{j+1}} d_{a,b} \lambda^{sr_j-sr_{j-1}+sl_{j+1}-sl_j} \lambda^{b-sr_j-1} \lambda^{b-sr_{j-1}-sl_{j+1}+sl_j} + \dots + \\
& \left. \sum_{b=sr_{k-1}+1}^{sr_k} d_{a,b} \lambda^{sr_{k-1}-sr_{j-1}+sl_k-sl_j} \lambda^{b-sr_{k-1}-1} \lambda^{b-sr_{j-1}-sl_k+sl_j} \right) = \\
& \lambda^{a-1-sl_{j-1}} \cdot \lambda^{sr_{j-1}-sl_j+sl_1} \sum_{b=sr_{j-1}+1}^{sr_k} d_{a,b} \lambda^{2(b-sr_{j-1})-1} \leq \\
& \lambda^{a-sl_{j-1}-1} \lambda^{sr_{j-1}-sl_j+sl_1-1} p_o(\lambda),
\end{aligned}$$

since at most o elements $d_{a,b}$ with fixed a are equal to 1, and thus $M \cdot \Lambda \leq p_o(\lambda) \Theta$.

Similarly, the b -th element of $M^T \cdot \Theta$ (again with $sr_{j-1} < b \leq sr_j$ for a suitable $j > 0$) is equal to

$$\begin{aligned}
& \lambda^{b-sr_{j-1}-1} \left(\sum_{a=1}^{sl_1} d_{a,b} \lambda^{a-1} \lambda^{sr_{j-1}+sl_j-sl_1+1} \lambda^{a-1} + \right. \\
& \sum_{a=sl_1+1}^{sl_2} d_{a,b} \lambda^{a-sl_1-1} \lambda^{sr_{j-1}-sr_1+sl_j-sl_2+1} \lambda^{a-1-sl_1} \lambda^{sr_1-sl_2+sl_1} + \\
& + \dots + \sum_{a=sl_{j-1}+1}^{sl_j} d_{a,b} \lambda^{a-sl_{j-1}-1} \lambda \lambda^{a-1-sl_{j-1}} \lambda^{sr_{j-1}-sl_j+sl_1} \left. \right) = \\
& \lambda^{b-sr_{j-1}} \cdot \lambda^{sr_{j-1}-sl_j+sl_1-1} \left(\sum_{a=1}^{sl_1} d_{a,b} \lambda^{2(a+sl_j-sl_1)-1} + \right. \\
& \sum_{a=sl_1+1}^{sl_2} d_{a,b} \lambda^{2(a+sl_j-sl_2-sl_1)-1} + \dots + \sum_{a=sl_{j-1}+1}^{sl_j} d_{a,b} \lambda^{2(a-sl_{j-1})-1} \left. \right) \leq \\
& \lambda^{b-sl_j+sl_1-1} p_i(\lambda),
\end{aligned}$$

param. d	2	3	4	5	6	7	8	9
$g(d)$	1.5728	1.4829	1.4555	1.4459	1.4425	1.4412	1.4407	1.4405

Figure 6: General lower bound for different values of the parameter d . $t \geq g(d)(\log n) - O(\log \log n)$. For limited d no previous lower bounds known (except the ones inferred from broadcasting in [16, 3]), while for $d = \infty$ the value coincides with the one in [5, 15, 14, 19].

since at most i elements $d_{a,b}$ with fixed b are equal to 1.

Thus, $M^T \cdot \Theta \leq p_i(\lambda)\Lambda$ and

$$M^T \cdot M \cdot \Lambda \leq p_o(\lambda)M^T \Theta \leq p_i(\lambda)p_o(\lambda)\Lambda,$$

hence the lemma. \square

>From Lemma 5.1, Lemma 5.2 and Lemma 5.3, the following theorems hold.

Theorem 5.4 *Let $\langle A_1, \dots, A_t \rangle$ be an (i, o) -restricted gossip protocol for a digraph $G = (V, A)$. Then $t \geq g(i, o)(\log n) - O(\log \log n)$, where $n = |V|$, $g(i, o) = \frac{1}{(\log 1/\lambda)}$ and λ is a positive real number such that $\sqrt{p_i(\lambda)}\sqrt{p_o(\lambda)} = 1$.*

Theorem 5.5 *Let $\langle A_1, \dots, A_t \rangle$ be an (i, o) -restricted gossip protocol for a digraph $G = (V, A)$ with an $\langle \alpha, l \rangle$ -separator. Then $t \geq g(i, o)(\log n)(1 - o(1))$, where $g(i, o) = \max_{\lambda \mid \sqrt{p_i(\lambda)}\sqrt{p_o(\lambda)} \leq 1} l \left(\frac{\alpha - (\log \sqrt{p_i(\lambda)}\sqrt{p_o(\lambda)})}{(\log 1/\lambda)} \right)$.*

As a consequence of Theorem 5.4, Theorem 5.5, Lemma 3.1 and Lemma 3.3, new lower bounds can be determined for general and specific network topologies.

Corollary 5.6 *Let $G = (V, A)$ be a digraph with fixed parameter $d > 1$. Then any directed or half-duplex gossip protocol for G takes $t \geq g(d)(\log n) - O(\log \log n)$ steps, where $n = |V|$, $g(d) = \frac{1}{(\log 1/\lambda)}$ and λ is a positive real number such that $\sqrt{p_\infty}\sqrt{p_d(\lambda)} = 1$.*

Some numerical bounds arising from Corollary 5.6 are listed in Figure 6.

Corollary 5.7 *The lower bounds on the gossiping time of any protocol for $BF(d, D)$, $W\tilde{B}F(d, D)$, $WBF(d, D)$, $DB(d, D)$ and $K(d, D)$ in Figure 7 hold.*

period ∞	ours	previous
$g(BF(2, D))$	2.4200	2.4193 [6]
$g(BF(3, D))$	1.7889	1.7788 [6]
$g(W\vec{B}F(2, D))$	2.4280	2.4193 [6]
$g(W\vec{B}F(3, D))$	1.7825	1.7788 [6]
$g(W\vec{B}F(4, D))$	1.5895	1.5876 [6]
$g(W\vec{B}F(5, D))$	1.5071	1.5060 [6]
$g(WBF(2, D))$	1.9770	1.9750 [6]
$g(WBF(3, D))$	1.5544	1.5538 [6]
$g(WBF(4, D))$	1.4591	1.4589 [6]
$g(\vec{DB}(2, D))$ and $g(\vec{K}(2, D))$	1.6375	1.5876 [6]
$g(DB(2, D))$ and $g(K(2, D))$	1.5965	1.5876 [6]

Figure 7: Some improved lower bounds for specific networks. Values have to be multiplied times $(\log n)(1 - o(1))$. The unlisted entries coincide with the ones in Figure 6 or in [6].

6 Extensions and Generalizations

We now briefly sketch how our results can be extended to other models. In all the cases our lower bound technique can be used as well, with the difference that the norm of the matrix associated to the protocol is different. Even if we don't show numerical values, all the results for general and specific topologies can be extended by using the new norm.

Let us consider first the c -port model. In this case the condition that only one incident arc can be active at each round is relaxed by admitting at most a given number $c > 0$ of active arcs.

For broadcasting and (thus full-duplex gossiping) it means that given any incoming activation at a given vertex, then there are still at most o outgoing activations influenced, where o is the output restriction. However, not all such outgoing activations have a different delay, since up to c of them can belong to the same round. Hence, if $o = q \cdot c + r$, then $\|M(\lambda)\|_\infty \leq c\lambda + c\lambda^2 + \dots + c\lambda^q + r\lambda^{q+1}$.

Similar considerations hold for the directed and half-duplex gossiping. Here each row can contain at most c equal entries and the same holds for each column. By the (i, o) -restriction, a completely analogous argument shows that $\|M(\lambda)\| \leq$

$\sqrt{(c\lambda + c\lambda^3 + \dots + c\lambda^{2q_i-1} + r_i\lambda^{2q_i+1})} \sqrt{(c\lambda + c\lambda^3 + \dots + c\lambda^{2q_o-1} + r_o\lambda^{2q_o+1})}$, where $i = q_i \cdot c + r_i$ and $o = q_o \cdot c + r_o$.

In the postal model there is an additional integer parameter $\delta > 0$ such that, once a given item has been sent through a link, it will be available at the arriving vertex to be sent on another link only after δ rounds (hence $\delta = 1$ in the basic model). This means that an incoming activation cannot influence the outgoing activations before the next δ rounds and thus all the entries of $M(\lambda)$ are either 0 or λ^x with $x \geq \delta$. By completely analogous observations it is then easy to see that both in broadcasting and in directed and half-duplex gossiping (also under c -port) it is sufficient to multiply the basic norm by $\lambda^{\delta-1}$.

Notice that using the above norms new lower bounds can be obtained for all the restricted protocols and thus for the bounded degree and also systolic ones.

7 Conclusion

In this paper we have provided new lower bounds for restricted broadcasting and gossiping protocols. As a consequence new lower bounds have been determined for bounded degree networks in the general case and for specific topologies. Moreover as a corollary we obtain the same results for systolic protocols in [6].

Another example of restricted protocols are the “memoryless” ones, where fixed a given number of steps $\delta > 0$, every vertex remembers only the items received during the previous δ steps. This means that an incoming activation influences at most δ successive outgoing activations and an outgoing activation depends on at most δ previous incoming activations, i.e. the protocol is (δ, δ) -restricted.

We believe that memoryless protocols are not just an artificial example of restricted protocols, but they might be useful to improve the lower bounds for bounded degree networks. In fact, it seems that in this case the input-output restriction is a too local property to allow the determination of the best possible lower bound, that we conjecture to be the one corresponding to a (d, d) -restriction. Locally at each vertex it is possible to establish only a (∞, d) -restriction, but it seems that the best dissemination time is achieved when the vertices have an equal alternance of input and output activations, so that in the average also the input restriction is low. A way to limit the input activation is that of resorting to more global properties. We conjecture in fact that in a network with fixed parameter d memoryless protocols with $\delta \approx d$ are able to reach the optimal time up to a negligible additive factor. If this is true, then the better lower bounds for bounded degree networks can be easily accomplished.

References

- [1] A. Berman and R.J. Plemmons. *Nonnegative matrices in the mathematical science*. Classics in Applied Mathematics. SIAM, 1994.
- [2] J.C. Bermond, L. Gargano, A. Rescigno, and U. Vaccaro. Fast gossiping by short messages. *SIAM Journal on Computing*, 27:917–941, 1998.
- [3] J.C. Bermond, P. Hell, A.L. Liestman, and J.G. Peters. Broadcasting in bounded degree graphs. *SIAM Journal on Discrete Maths*, 5(1):10–24, 1992.
- [4] Jean de Rumeur. *Communication dans les réseaux de processeurs*. Collection Etudes et Recherches en Informatique. Masson, 1994. (English version to appear).
- [5] S. Even and B. Monien. On the number of rounds necessary to disseminate information. In *1st ACM Symposium on Parallel Algorithms and Architectures (SPAA)*, pages 318–327, 1989.
- [6] M. Flammini and S. Pérennès. Lower bounds on systolic gossip. Manuscript submitted for the publication. A preliminary version appears in *Proc. of the 11th IEEE International Parallel Processing Symposium*, 1997.
- [7] P. Fraigniaud and E. Lazard. Methods and problems of communication in usual networks. *Discrete Applied Mathematics*, 53(1-3):79–133, 1994.
- [8] S.M. Hedetniemi, S.T. Hedetniemi, and A.L. Liestman. A survey of gossiping and broadcasting in communication networks. *Networks*, 18:319–349, 1986.
- [9] J. Hromkovič, R. Klasing, E. Stohr, and H. Wagener. Gossiping in vertex-disjoint paths mode in d-dimensional grids and planar graphs. *Information and Computation*, 123(1):17–28, 1995.
- [10] J. Hromkovič, R. Klasing, W. Unger, and H. Wagener. Optimal algorithms for broadcast and gossip in the edge-disjoint path modes. *Information and Computation*, 133(1):1–33, 1997.
- [11] J. Hromkovič, R. Klasing, B. Monien, and R. Peine. Dissemination of information in interconnection networks (broadcasting and gossiping). In Ding-Zhu Du and D. Frank Hsu (eds.): *Combinatorial Network Theory*, Kluwer Academic Publishers, pages 125–212, 1995.

- [12] J. Hromkovič, R. Klasing, D. Pardubská, W. Unger, and H. Wagener. The complexity of systolic dissemination of information in interconnection networks. *R.A.I.R.O. Theoretical Informatics and Applications*, 28(3-4):303–342, 1994.
- [13] R. Klasing, B. Monien, R. Peine, and E. Stohr. Broadcasting in butterfly and de Bruijn networks. *Discrete Applied Mathematics*, 53(1-3):183–197, 1994.
- [14] D. W. Krumme, G. Cybenko, and K. N. Venkataraman. Gossiping in minimal time. *SIAM J. Comp.*, 21(1):111–139, 1992.
- [15] R. Labahn and I. Warnke. Quick gossiping by multi-telegraphs. *Topics in Combinatorics and Graph Theory*, pages 451–458, 1990.
- [16] A.L. Liestman and J.G. Peters. Broadcast networks of bounded degree. *SIAM Journal on Discrete Maths*, 1(4):531–540, 1988.
- [17] S. Pérennès. *Communications dans les réseaux d’interconnexion*. PhD thesis, Université de Nice - Sophia Antipolis, Laboratoire d’Informatique, Signaux et Systèmes de Sophia Antipolis CNRS URA 1376, 1996.
- [18] S. Pérennès. Lower bounds on broadcasting time of de Bruijn networks. In Springer-Verlag, editor, *2nd Int. Euro-Par Conference*, volume 1123, pages 325–332. Lecture Notes in Computer Science, 1996.
- [19] V.S. Sunderam and P. Winkler. Fast information sharing in a complete network. *Discrete Applied Mathematics*, 42:75–86, 1993.



Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)

Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)

Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)

Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
<http://www.inria.fr>
ISSN 0249-6399